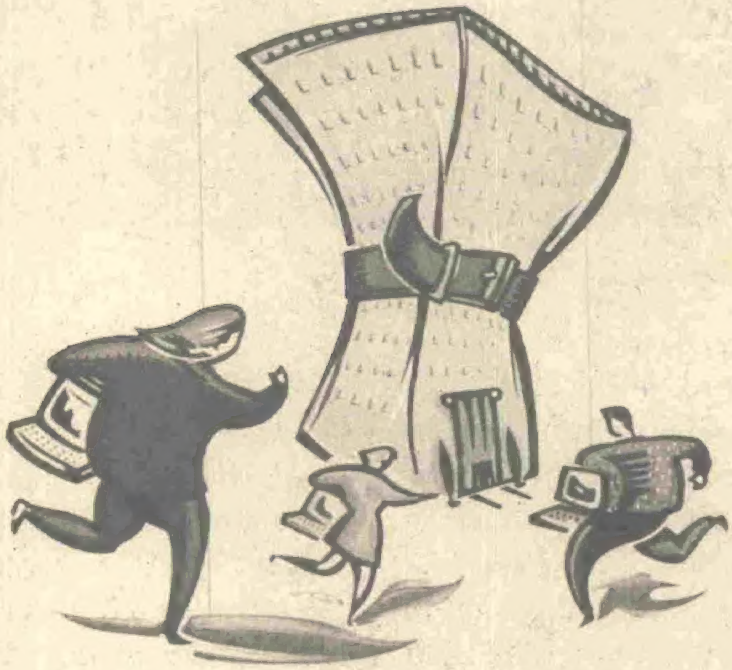
เอนก ศิรจริยาภิวัฒน์

หนทางต่อสู้และป้องกันไวรัส
Diskmon

หัวใจของการทำงานคือข้อมูล เพื่อรักษาความปลอดภัย ของข้อมูลไม่ให้ได้รับอันตราย โปรแกรมคอมพิวเตอร์ช่วยคุณได้



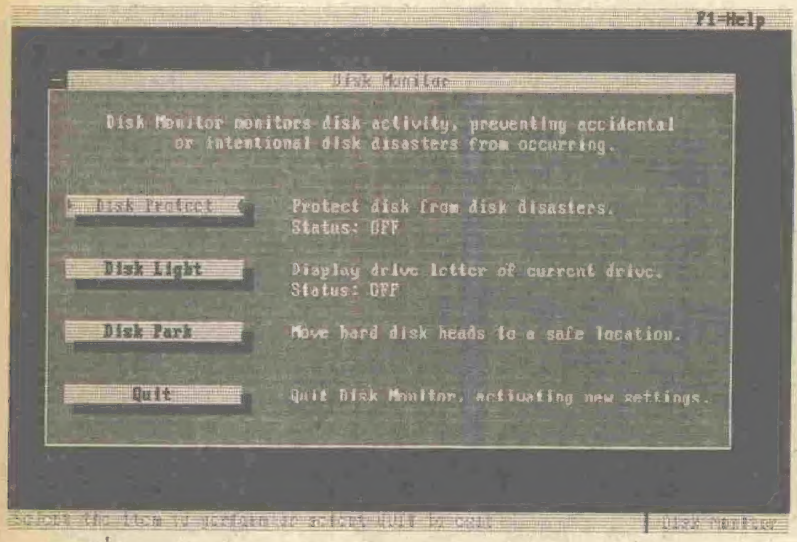
ในฉบับที่แล้วเราได้นำเสนอบทความในการป้องกันการสูญหายของข้อมูลโดยใช้ Erase protect เราจะเห็นว่าด้วย Erase protect เราจะสามารถกู้ข้อมูลที่ถูกลบทิ้งกลับมาได้อย่างมีประสิทธิภาพ โปรแกรมต่าง ๆ ในนอร์ตันยูทิลิตี้มีหลาย ๆ โปรแกรมที่มีประโยชน์ในการป้องกันการเสียหายของโปรแกรมและข้อมูล โดยเฉพาะข้อมูลเกี่ยวกับระบบ (system file and system data) ซึ่งหลายครั้งที่ข้อมูลเหล่านี้หายไปหรือสูญเสียไป ทำให้ระบบทำการบูตไม่ได้ เราจึงจำเป็นต้องเก็บข้อมูลส่วนนี้ไว้ ซึ่งโปรแกรมนอร์ตันยูทิลิตี้จะเก็บส่วนนี้ไว้บนดิสก์ (Rescue Disk) นอกจากนั้นยังมีโปรแกรมอีกหลาย ๆ ตัวซึ่งท่านผู้อ่านสามารถอ่านได้จากบทความเรื่อง กู้ไฟล์กับ Norton Utilities 5.0 ของคุณกิติพงษ์ ฤทธิบุตร ซึ่งมี 2 ตอนจบ ส่วนมุมหนทางต่อสู้และป้องกันไวรัสคราวนี้จะเป็นการป้องกันและดูแลข้อมูลที่เก็บอยู่ในดิสก์โดยใช้โปรแกรม diskmon

Diskmon ทำอะไรได้บ้าง

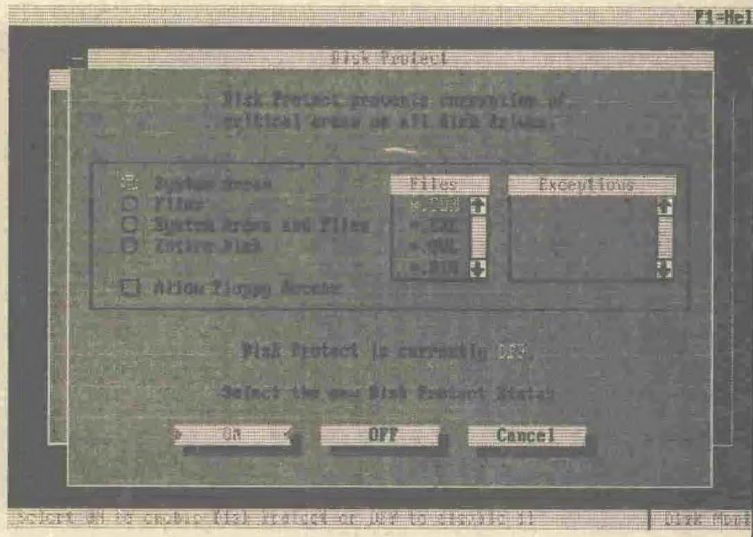
โปรแกรม Diskmon จะดูแลข้อมูลไม่ให้สูญหายไปเนื่องจากอุบัติเหตุหรือจากวัตถุประสงค์ร้าย (เช่นจากไวรัส) ซึ่งจะมีการทำงานอยู่ 3 ส่วนด้วยกันคือ Disk Protect, Disk Light และ Disk Park

1. Disk Protect จะทำหน้าที่ป้องกันการเขียนข้อมูลโดยเราไม่ได้รับอนุญาตให้เขียน (ซึ่งเป็นวิธีการทำงานสำคัญของไวรัสต่าง ๆ) เราสามารถป้องกันส่วนของระบบ (system areas) ไฟล์ข้อมูลต่าง ๆ หรือป้องกันการเขียนทั้งหมด การป้องกันนี้สามารถป้องกันการลบข้อมูลหรือเขียนข้อมูลทับไฟล์สำคัญ ๆ ได้

2. Disk Light จะแสดงว่าเรากำลังติดต่อหรือใช้ข้อมูลจากไดรฟ์ไหนโดยแสดงสัญลักษณ์, พร้อมชื่อไดรฟ์บริเวณมุมบนขวาของจอภาพ (ยกเว้นการแสดงผลในกราฟิกโหมด) การแสดงว่าเรากำลังทำงานไดรฟ์ใดอยู่นี้เป็นสิ่งที่ดีกับเรา เพราะ จะเป็นการป้องกันการดึงเอาดิสก์ออกจากไดรฟ์ก่อนที่จะเขียนข้อมูลเสร็จหรือการปิดเครื่องโดยเขียนข้อมูลยังไม่เสร็จ ซึ่งเป็นสาเหตุของอาการผิดปกติของข้อมูลมากมาย เช่น ไฟล์มีขนาดเหลือศูนย์ไบต์ (เนื่องจากยังไม่มีการปิดไฟล์ จึงไม่มีการเขียนข้อมูลลงไฟล์นั้นเลย), ข้อมูลบางส่วนหายไป (เกิดจากการเขียนข้อมูลไม่ครบ), การเกิด cross link, lost chain ...ฯลฯ



รูปที่ 1 เมนูหลักของ Diskmon



รูปที่ 2 การใช้ Disk Protect

3. Disk Park ฮาร์ดดิสก์ทุกตัวจะมีส่วนที่พักหัวอ่าน/เขียน (head park) ซึ่งฮาร์ดดิสก์รุ่นใหม่ ๆ จะสามารถนำหัวอ่าน/เขียนไปเก็บไว้บริเวณที่พักได้อย่างอัตโนมัติ (Auto Park) เมื่อเลิกใช้ฮาร์ดดิสก์ แต่ก็มีอยู่หลายรุ่นที่ไม่ได้ทำการพักหัวอ่าน/เขียนให้เราอย่างอัตโนมัติ จึงเป็นหน้าที่ของเราที่จำเป็นต้องสั่งให้มีการเก็บหัวอ่าน/เขียนไว้ที่พัก (Park Zone) เป็นการป้องกันการกระแทกหัวอ่าน/เขียนกับแผ่นดิสก์ การเสียหายจากสาเหตุอื่น (เช่น มีไฟกระชากมาที่บริเวณหัวอ่าน/เขียน อาจทำให้เกิดข้อมูลที่ไม่ต้องการได้) ขณะที่เราปิด/เปิดเครื่องและการเก็บหัวอ่าน/เขียนไว้ที่พักนี้จำเป็นมากเมื่อเราจะทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์ของเรา

การใช้ Diskmon ผ่านระบบเมนู

เราสามารถใช้งานโปรแกรมทั้ง 3 ส่วนของ Diskmon โดยผ่านเมนูของ Diskmon โดยการเรียกโปรแกรม Diskmon จะเกิดเมนูดังรูปที่ 1 ซึ่งเราจะเลือกการทำงานทั้ง 3 ส่วนได้ตามต้องการ

1. Disk Protect (รูปที่ 2) เราสามารถกำหนดการป้องกันส่วนต่าง ๆ ได้ดังนี้

- system area จะป้องกันการเขียน Partition table, Boot record และ system file จากโปรแกรมต่าง ๆ (ยกเว้น Norton Disk Editor)

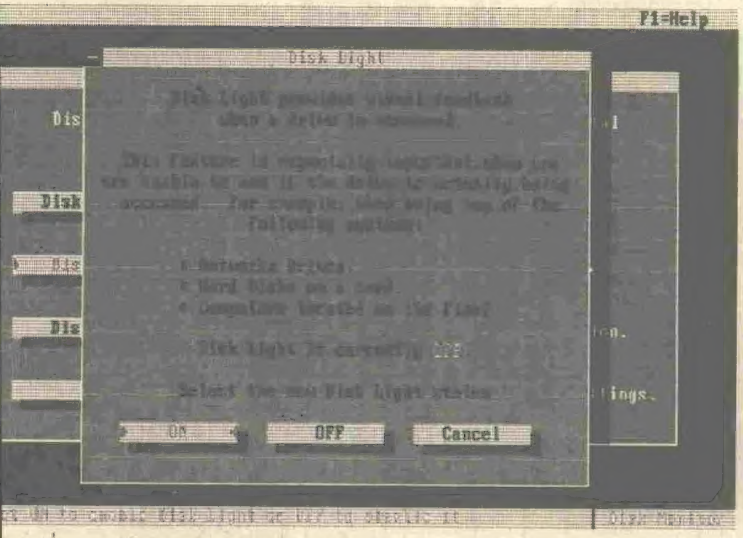
- files จะทำการป้องกันการเขียนไฟล์ ซึ่งจะรวมถึงการลบไฟล์ทิ้งและการเปลี่ยนแปลงแก้ไขไฟล์ (ไม่ป้องกันการก๊อบปี้ไฟล์ใหม่เข้าสู่ดิสก์) ไฟล์นามสกุลต่าง ๆ ที่จะป้องกันเราสามารถระบุได้ในกล่อง (list box) ของไฟล์ โดยกล่องของไฟล์นี้จะมีนามสกุล .COM, .EXE, .OVL, .BIN และ .SYS ให้อยู่แล้ว สำหรับกล่องยกเว้น (exceptions box) จะเป็นการระบุว่าไฟล์ใดบ้างที่ไม่ต้องการทำการป้องกัน เช่น ต้องการป้องกันไฟล์นามสกุล .COM ทุกไฟล์ยกเว้น SK.COM รายชื่อไฟล์ในกล่องไฟล์ก็จะมี *.COM ในกล่องไฟล์ยกเว้นก็จะมี SK.COM ในกล่องยกเว้น (exception box) นี้สามารถระบุชื่อไฟล์ได้มากสุด 20 แบบ (ใช้คำว่า แบบ เพราะว่าเราสามารถระบุในลักษณะ WILD CARD ได้เช่น S*.COM คือยกเว้นไฟล์นามสกุล .COM ทุกไฟล์ที่ขึ้นต้นชื่อไฟล์ด้วยอักษร S)

- system areas and files ป้องกันทั้ง 2 ส่วนที่กล่าวมาข้างต้น

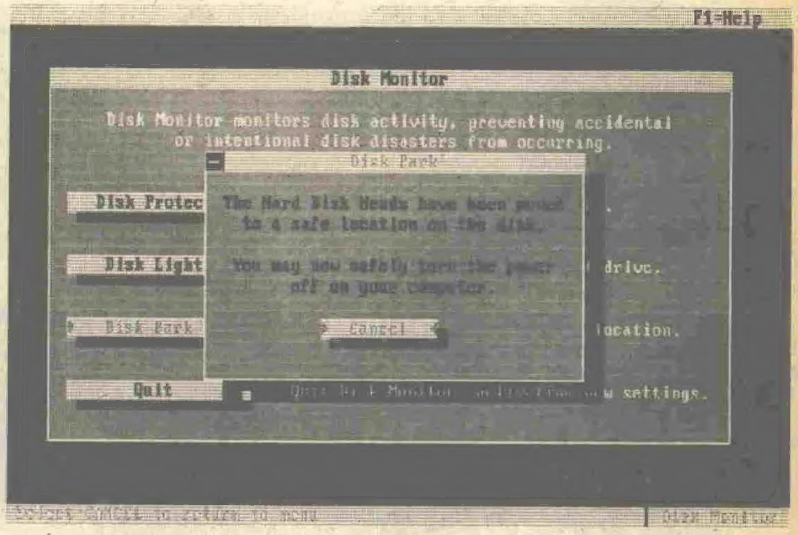
- entire disk จะทำการป้องกันการเขียนทุกอย่าง (แม้จะเป็นการก๊อบปี้ไฟล์ก็ตาม)

- allow floppy access เป็นตัวระบุว่าจะยกเว้นการป้องกันฟลอปปี้ดิสก์หรือไม่ ซึ่งการเลือกหัวข้อนี้จะทำให้การฟอร์แมตแผ่นฟลอปปี้ดิสก์เป็นไปอย่างราบรื่น มิฉะนั้นจะมีการถามจาก Diskmon ตลอดเวลา ซึ่งสร้างความรำคาญให้ผู้ใช้

2. Disk Light (รูปที่ 3) เราเลือกว่าจะมีการแสดง (ON) ชื่อไดรฟ์หรือไม่แสดง (OFF) เราจะสังเกตได้จากรูปว่า การใช้ Disk Light มีประโยชน์มากกับดิสก์ที่เป็นเน็ตเวอร์ก, ฮาร์ดดิสก์ที่อยู่บนการ์ดและคอมพิวเตอร์ที่ตั้งไว้ที่พื้น (หรือวางไว้ใต้โต๊ะ ซึ่งส่วนมากจะเป็นแบบซึ่งเรียกว่า towel



รูปที่ 3 การใช้ Disk Light



รูปที่ 4 การเก็บหัวอ่าน/เขียน

```
C:\UTIL>diskmon /?
Disk Monitor, Norton Utilities 6.01, Copyright 1991 by Symantec Corporation

Protect disks from accidental or malicious damage.

DISKMON [/PROTECT+|-] [/LIGHT+|-] [/SKIPHIGH]
DISKMON /STATUS
DISKMON /UNINSTALL
DISKMON /PARK

  /PROTECT+|-     Enable or disable Disk Protect.
  /LIGHT+|-       Enable or disable Disk Light.
  /SKIPHIGH       Do not load into High memory.
  /STATUS         Display Disk Monitor Status.
  /UNINSTALL      Uninstall Disk Monitor.
  /PARK           Park heads on all drives.

C:\UTIL>
```

รูปที่ 5

case) เพราะดิสก์เหล่านี้เราจะไม่เห็นไฟ (LED) ซึ่งแสดงการทำงานของไดรฟ์ แต่ใช่ว่าคอมพิวเตอร์ที่ตั้งบนโต๊ะจะไม่มีประโยชน์นะครับ เพราะเป็นตัวช่วยดูการทำงานของไดรฟ์ได้เป็นอย่างดี เพื่อป้องกันข้อมูลของเราเกิดการเสียหายดังที่กล่าวมาข้างต้น

3. Disk Park (รูปที่ 4) เมื่อเลือกเมนูนี้ก็พร้อมที่จะปิดเครื่องและทำการเคลื่อนย้ายคอมพิวเตอร์ ถ้าเราต้องการยกเลิกการเก็บหัวอ่าน/เขียน ให้กด Enter ซึ่งจะเป็นการเลือกการยกเลิก (Cancel) การเก็บหัวอ่าน/เขียน ซึ่งเราจะใช้งานคอมพิวเตอร์ของเราได้อย่างปกติต่อไป

การใช้ Diskmon ผ่านบรรทัดคำสั่ง (command line)

การสั่งให้ Diskmon ทำงานโดยไม่ต้องแสดงเมนู เราสามารถกระทำได้โดยการสั่ง Diskmon ตามด้วยพารามิเตอร์ที่เราต้องการ (รูปที่ 5) เช่น ต้องการเก็บหัวอ่าน/เขียน เราใช้

```
Diskmon/park
```

ถ้าต้องการพารามิเตอร์หลาย ๆ ตัวเราก็สั่งต่อเนื่องกันไป เช่น ต้องการทำการป้องกันไดรฟ์จากการเขียน แต่ไม่ต้องการแสดงชื่อไดรฟ์ที่ติดต่อที่มุมขวาบน เราใช้

```
Diskmon/protect + /Light-
```

สำหรับการป้องกันการเขียน (Protect) เราจะระบุเงื่อนไขต่าง ๆ ผ่านระบบเมนู ซึ่งข้อมูลต่าง ๆ จะถูกเก็บไว้ในไฟล์ Diskmon.ini ทำให้เราใช้เงื่อนไขต่าง ๆ เหล่านั้นได้ภายหลังโดยไม่จำเป็นต้องแสดงเมนูอีก สำหรับการใช้ป้องกันการเขียน (Protect) เราจำเป็นต้องยกเลิก เมื่อต้องการใช้โปรแกรมที่มีการเขียนข้อมูลลงดิสก์ เช่น ไมโครซอฟต์วินโดวส์ เมื่อเราใช้ซอฟต์แวร์เหล่านี้บ่อย ๆ เราควรจะเขียนเป็นแบตช์ไฟล์ไว้เรียกใช้ เพื่อความสะดวกในการติดตั้ง Diskmon ตัวอย่างแบตช์ไฟล์ของไมโครซอฟต์วินโดวส์ (windows.bat) เป็นดังนี้

```
Diskmon/Protect-
WIN
Diskmon/Protect +
```

การใช้ Diskmon จะมีวิธีการใช้ดังที่กล่าวมา จะเห็นว่าโปรแกรม Diskmon ตัวนี้จะช่วยให้ข้อมูลได้รับความปลอดภัยของเพิ่มขึ้น แล้วจะไม่ลองใช้กันดูบ้างหรือครับ